



# The Security Development Lifecycle (SDL)

**Security Engineering & Communications**

# Overview



- Security Development Lifecycle (SDL) formalizes security best practices from Windows Server 2003, .NET Framework v1, other security pushes of late 2001, early 2002
  - Development process
    - Threat modeling
    - Security Push
    - Final Security Review (FSR) – formerly security audit
  - Security education
- SDL is a best practice mandated by SteveB & SLT. Properly implemented, it will produce the best more secure products possible for our customers
  - Process
  - Education
  - Accountability

Process	Education	Accountability
<ul style="list-style-type: none"><li>• Defined milestones tied to product lifecycle</li><li>• New resources<ul style="list-style-type: none"><li>– SWI buddy</li><li>– Guidance and tools</li></ul></li><li>• New deliverables<ul style="list-style-type: none"><li>– Early threat models</li><li>– Fuzz testing</li></ul></li></ul>	<ul style="list-style-type: none"><li>• Annual engineer training</li><li>• Tracking of training compliance</li><li>• On-line training options</li><li>• Specialized training options</li></ul>	<ul style="list-style-type: none"><li>• Business group CPE metrics by product</li><li>• Training metrics by organization</li></ul>

# Security Engineering Background



<b>How we got here</b>	<ul style="list-style-type: none"><li>• Security push or stand down originated with .NET Framework 1.0 and Windows Server 2003</li><li>• Final Security Review (FSR) by SWI team initiated before Windows Server 2003 RTM. FSR proves effective</li><li>• Security push and FSR extended to other products</li></ul>
<b>What product teams have done</b>	<ul style="list-style-type: none"><li>• Develop threat models to focus security analysis, code review, attack testing on the high risk areas</li><li>• Follow guidelines on coding, testing, tool usage</li><li>• Conduct a security push at code complete (after Beta 1)</li></ul>
<b>What SWI team has done (key components)</b>	<ul style="list-style-type: none"><li>• Maintain a web repository of tools and guidance (<a href="http://swi">http://swi</a>)</li><li>• Answer questions on security development practices</li><li>• Conduct FSR</li><li>• Investigate reported security vulnerabilities and initiate "security response lockdown" for systemic/major issues</li></ul>
<b>What we've achieved</b>	<ul style="list-style-type: none"><li>• Over fifty security pushes and forty FSRs across Microsoft; over 100 total engagements including consulting, reviews, training; over 100 patch-class issues found during FSRs</li><li>• Over 10,000 engineers trained across Microsoft (most during Windows Server 2003 security push)</li><li>• Products that pushed through the process are measurably more secure</li></ul>

## Impact of Security Engineering on Products



Critical or important vulnerabilities in the first...

...270 days    ...365 days    TwC release?

Windows XP Service Pack 3	36	42	No
Windows XP Service Pack 3	6	13	Yes

**Critically important to review "old code"**

# SDL Process



# SDL Education



<b>Education Focus</b>	<b>Mandatory training &amp; education:</b> <ul style="list-style-type: none"><li>• Mandatory 4-hour training for all engineers<ul style="list-style-type: none"><li>- Applies to Dev, Test, PM, QA, UE assigned to products where SDL is mandatory</li><li>- Required if previous training was prior to 1 October 2003</li><li>- Will be offered at major remote development sites</li></ul></li><li>• On-line training option under development<ul style="list-style-type: none"><li>- Appropriate for remote sites</li><li>- May be alternative to live training</li></ul></li><li>• Specialized course offerings will satisfy mandatory training requirement</li></ul>	<ul style="list-style-type: none"><li>• Targeted for completion by 7/04</li><li>• In final editing now</li><li>• In planning – to roll out in FY05</li></ul>
<b>Accountability for learning</b>	<b>Track and evaluate engineer training</b> <ul style="list-style-type: none"><li>• Record all engineer training</li><li>• Develop improved training transcript system</li><li>• Develop employee training assessment system</li><li>• Reflect training level (classes, assessment) in reviews, promotion, assignments</li></ul>	<ul style="list-style-type: none"><li>• Now</li><li>• Begins FY05</li><li>• Begins FY05</li><li>• Begins FY05</li></ul>



## Planned Additions to SDL



- **Change process**
  - SDL process documents updated as needed
  - SDL requirements updated twice yearly
  - New requirements posted as "recommendations" three months before effective date
- **Current plans**
  - Training updates and accountability
  - Security architecture and Trusted Computing Base
  - Defining and measuring attack surface
  - Privacy requirements
  - Integrated process as alternative to security push





## Demonstration/Questions